

## Office of Financial Institutions AUTHENTICATION

### **I. Purpose:**

Access to data or resources in a computer system with the most basic level of security most often requires the user to identify him/her-self and prove his/her identity. The user's identification (user-ID) tells the system who the user is and the user's password proves, or authenticates, the user's identity. Once the system knows who the user is, it can determine what data and resources the user can access.

Authentication focuses on something you know (passwords, PIN), something you have (digital tokens, smart cards) and something you are (biometrics). Any combination of these can be used to authenticate a user. Most computer systems rely on a user-ID and password for authentication. However, authentication can be much more secure when these methods are combined.

Information is a state asset that must be protected from unauthorized access, use, modification and destruction. The authentication process provides protection by controlling access to the assets of information technology systems. Authentication techniques permit validation of user's identities, hardware devices, and/or transmitted information.

### **II. Policy:**

OFI will use at least one of the following methods of authentication when accessing or utilizing state-owned or managed information technology systems.

- A. Passwords - OFI will establish and implement criteria governing one of the following:
  - a. A reasonable number (3-5) of unsuccessful login attempts allowed prior to revocation of password.
  - b. Maximum validity periods for passwords to be no greater than 31 days, with specific exemptions granted for special purposes such as enabling a stored procedure to run against a database.
  - c. Passwords shall be kept confidential.
  - d. Minimum password length and format shall be no less than eight (8) characters.
  - e. Minimum password complexity should contain at least 3 of the 4 categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and non-alphanumeric characters (%,&,!).

**Office of Financial Institutions  
AUTHENTICATION**

- f. Passwords shall not be kept on paper or stored in plain text format.
  - g. All passwords shall be changed whenever it is determined that a system's security may have been compromised.
  - h. Passwords shall be changed on a regular basis and the cycling or re-use of passwords will be reasonably limited. Applicable devices and application systems shall maintain a password history file to prevent continual reuse of the same passwords or group of passwords for a valid user-ID (with 3 being the minimum number of previous passwords checked), where the capability exists.
  - i. Passwords must not be hard coded into software.
  - j. Passwords must not be stored in dial-up communications utilities or browsers.
  - k. Passwords must not be recorded in a system log unless the password is encrypted.
  - l. Passwords must not be stored in any file, program, command list, procedure, macro, script or function key where it is susceptible to disclosure or to automate the log in process.
  - m. Temporary or "reset" passwords shall be changed upon first use.
- B. Biometrics - Refers to technologies for measuring and analyzing human body characteristics especially for authentication purposes.
- C. Biometric authentication methods are:
- a. Finger scan (fingerprints)
  - b. Hand geometry
  - c. Iris and retina scans
  - d. Facial scans
  - e. Voice recognition
- D. Biometric authentication systems deployed must meet accepted industry standards in order to maximize long term cost effectiveness and for ease of integration. Accepted file formats are:

**Office of Financial Institutions  
AUTHENTICATION**

- a. HA – API
  - b. Bio – API
  - c. CBEFF
  - d. Speech applications must comply with the SAPI standard.
- E. Smart Cards - Must provide a common, interoperable set of extended services and corresponding interfaces that support:
- a. Physical and logical access control
  - b. Biometrics
  - c. Cryptographic services, including digital signatures and PKI
- F. Smart card solutions must meet cryptographic standards set by:
- a. The National Institute of Standards and Technology
  - b. The National Security Agency
  - c. Federal Information Processing Standards Publication 46-3
- G. PKI - Public Key Infrastructure (PKI) is a combination of software, hardware, policies and procedures. A public key infrastructure (PKI) enables unsecured public networks such as the Internet, to securely and privately exchange data through the use of public and private cryptographic key pairs that are obtained and shared through a trusted authority.
- H. PKI standard is the X standard prepared by the International Telecommunication Union (ITU) X.509 Version 3.
- a. Minimum security services to be provided by this technology:
  - b. Encrypted information exchange (a minimum of 128 bit encryption)
  - c. Information integrity
  - d. Strong authentication
  - e. Digital signature

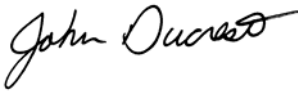
**Office of Financial Institutions  
AUTHENTICATION**

- f. Legal security controls
- g. Interoperability with different platforms, applications and domains

**III. Scope:**

OFI under the authority of the Office of Information Technology pursuant to the provisions of R.S. 39:15.1, et seq. will comply with this policy.

**APPROVED BY:**



---

**John Ducrest, CPA  
Commissioner**

May 9, 2008

---

**Date**

*This information was extracted in part from the Office of Information Technology Policy  
IT-POL-006 Authentication.*